IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	Moghe, Pratyush
Serial Number:	10/780,252
Filing Date:	February 17, 2004
Art Unit:	2134
Examiner:	Jung, David Yiuk
For:	**A method and apparatus to detect unauthorized information disclosure via content anomaly detection**

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF

This Brief is submitted pursuant to 37 CFR 41.37.

(i) Real Party In Interest. The real party in interest on this appeal is Tizor Systems, Inc., the assignee of record.[1]

(ii) Related Appeals and Interferences. There are no prior and pending appeals, judicial proceedings or interferences known to the appellant that may be related to, directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

[1] In February 2009, Tizor Systems, Inc. was acquired by Netezza Corporation, which was acquired by International Business Machines Corporation (IBM) in November, 2010.

(iii) Status of Claims. The status of all the claims in the application is set forth in the following claim listing. Each of claims 1-29, 42-45, 47-49 and 52-53 is on appeal.

1. (rejected)
2. (rejected)
3. (rejected)
4. (rejected)
5. (rejected)
6. (rejected)
7. (rejected)
8. (rejected)
9. (rejected)
10. (rejected)
11. (rejected)
12. (rejected)
13. (rejected)
14. (rejected)
15. (rejected)
16. (rejected)
17. (rejected)
18. (rejected)
19. (rejected)
20. (rejected)

21. (rejected)

22. (rejected)

23. (rejected)

24. (rejected)

25. (rejected)

26. (rejected)

27. (rejected)

28. (rejected)

29. (rejected)

30. (cancelled)

31. (cancelled)

32. (cancelled)

33. (cancelled)

34. (cancelled)

35. (cancelled)

36. (cancelled)

37. (cancelled)

38. (cancelled)

39. (cancelled)

40. (cancelled)

41. (cancelled)

42. (rejected)

43. (rejected)

44. (rejected)

45. (rejected)

46. (cancelled)

47. (rejected)

48. (rejected)

49. (rejected)

50. (cancelled)

51. (cancelled)

52. (rejected)

53. (rejected)

(iv) Status of Amendments.

There are no un-entered amendments.

(v) Summary of Claimed Subject Matter.

The following is a concise explanation of the subject matter defined in each of the independent claims that are the subject of the appeal.

Claim 1 describes a method of performing an application layer semantic analysis to detect information access anomalies (Substitute Specification[2], page 3, lines 11-13). The method begins by capturing data packets (Substitute Specification, FIG. 1, element "CMAD"). The captured data packets are filtered to detect information content (Substitute Specification, at page 7, lines 6-14; FIG. 1, element 10). The method then processes

packets based on semantics of an application or protocol (Substitute Specification, at page 7, lines 15-25; FIG. 1, element 12), and a quantitative representation is derived (Substitute Specification, page 7, line 26, through page 8, line 3; FIG. 1, element 14). A content signature (FIG. 2, element 30) is then derived from the quantitative representation (Substitute Specification, page 8, lines 4-9; page 10, line 4, through page 11, line 4; FIG. 1, element 14). Thereafter, a prototypical model is derived, where the model includes a frequency view of a set of content signatures accessed by a given user (Substitute Specification, page 9, lines 3-8; FIG. 1, element 18). The set of content signatures are indicative of content that is changing over time (Substitute Specification, page 11, lines 20-23; FIG. 5). Finally, an application layer information access anomaly is detected by using a semantic analysis to detect a given deviation from the prototypical model (Substitute Specification, page 9, lines FIG. 1, element 20; page 12, line 6, through page 15, line 15; page 3, lines 11-13; page 7, line 16).

Claim 49 describes an apparatus (Substitute Specification, at page 3, line 9 and line 23; FIG. 1, generally) that comprises a processor, and a computer memory that stores computer program instructions (Substitute Specification at page 7, line 3). The instructions (Substitute Specification, page 3, line 9) are executed by the processor to perform a method of detecting an information access anomaly (Substitute Specification, at page 3, lines 23-24, page 4, lines 1-2). The method comprises three (3) basic steps, which begin by monitoring data packets indicative of changing content over time (Substitute Specification, page 7, lines 7-14; FIG. 2, CMAD, element 10). A prototypical model is then generated

---

[2] The Substitute Specification was filed October 12, 2004.

(Substitute Specification, at page 9, lines 3-8; FIG. 1, element 18). Finally, a semantic analysis is performed against the prototypical model to identify an application level information access anomaly (See, generally, Substitute Specification, page 9, lines FIG. 1, element 20; page 12, line 6, through page 15, line 15; page 3, lines 11-13; page 7, line 16).

Means-plus-function (MPF) structure

There are no MPF-style claim limitations in the pending claims.

(vi) Grounds of Rejection to be Reviewed on Appeal.

Group I – claims 1-29, 42-45 and 47-49

Whether the Examiner erred in finding that alleged admitted prior art ("APA") discloses explicitly or inherently each and every limitation of each of claims 1-29, 42-45 and 47-49?

Group II – claims 52 and 53

Whether the Examiner erred in finding that alleged admitted prior art ("APA") discloses explicitly or inherently each and every limitation of each of claims 52-53?

(vii) Argument.

The pertinent legal principles are straightforward.

As the Board noted in its recent precedential opinion in *Ex parte Frye*, 94 U.S.P.Q.2d 1072, (BPAI 2010), the Examiner has the initial burden to set forth the basis for any rejection so as to put the patent applicant on notice of the reasons why the applicant is not entitled to a patent on the claim scope that he or she seeks – the so called "*prima facie* case." *In re Oetiker*, 977 F.2d 1443, 1445 (Fed. Cir. 1992); *In re Piasecki*, 745 F.2d 1468, 1472 (Fed. Cir. 1984) (the initial burden of proof is on the USPTO "to produce the factual basis for its rejection of an application under sections 102 and 103"). (quoting *In re Warner*, 379 F.2d 1011, 1016 (CCPA 1967)).

Moreover, although PTO Rule 1.104(c)(3) permits the Examiner to reject a claim based on alleged admitted prior art (APA), that same Rule (at §1.104(c)(2)) expresses the important requirement that "the pertinence of each [prior art] reference, if not apparent, must be clearly explained."

In considering grounds of rejection, "every limitation in the claim must be given effect rather than considering one in isolation from the others." See, *In re Geerdes*, 491 F. 2d 1260, 1262-63 (CCPA 1974). Moreover, a rejection based on prior art cannot be based on speculations and assumptions. *In re Steele*, 305 F. 2d 859, 862 (CCPA 1962).

To establish anticipation, every element and limitation of the claimed invention must be found in a single prior art reference, arranged as in the claim. *Karsten Mfg. Corp. v. Cleveland Golf Co.*, 242 F.3d 1376, 1383 (Fed. Cir. 2001). Anticipation thus requires exact correspondence between a subject claim and the teaching of the reference. *Net*

MoneyIn, Inc. v. Verisign, Inc., 545 F.3d 1359, 1369 (Fed.Cir. 2008) ("unless a reference discloses within the four corners of the document not only all of the limitations claimed but also all of the limitations arranged or combined in the same way as recited in the claim, it cannot be said to prove prior invention of the thing claimed"). Although the literal wording need not be found in the reference, the elements must be arranged as required by the claim.

The claimed subject matter must be disclosed "clearly and unequivocally" in the reference. *In re Arkley*, 455 F.2d 586, 587 (CCPA 1972). Moreover, anticipation is not established if, in reading a claim on something disclosed in a reference, it is necessary to pick, choose and combine various portions of the disclosure, which according to the teachings of the reference, are not directly related to each other. *Id.,* 455 F.2d at 587-88.

The prior art reference must describe every limitation in a claim either explicitly or inherently. *In re Schreiber*, 128 F.3d 1473, 1477 (Fed. Cir. 1997). Inherent anticipation, however, cannot be based on possibilities or probabilities. *Akamai Tech., Inc. v. Cable & Wireless Internet Serv., Inc.*, 344 F.3d 1186, 1192 (Fed. Cir. 2003) ("A claim limitation is inherent in the prior art only if it is necessarily present in the prior art, not merely probably or possibly present."); *In re Robertson*, 169 F.3d 743, 745 (Fed. Cir. 1999) ("Inherent anticipation requires that the missing descriptive material is 'necessarily present,' not merely probably or possibly present, in the prior art").

"Absence from the reference of any claimed element negates anticipation." *Kloster Speedsteel AB v. Crucible, Inc.*, 793 F.2d 1565, 1571 (Fed.Cir.1986).

Group I – claims 1-29, 42-45 and 47-49

Given the Examiner's reliance on alleged APA, claim construction is a threshold question here. Claim construction, of course, must always precede the question of whether the claim, as properly construed, is anticipated or obvious. *Medichem, S.A. v. Rolabo, S.L.*, 353 F.3d 928, 933 (Fed. Cir. 2003). A claim term must be construed in context, not as a single element in isolation. *Hockerson-Halberstadt, Inc. v. Converse, Inc.*, 183 F.3d 1369, 1374 (Fed. Cir. 1999); *ACTV, Inc. v. Walt Disney Co.*, 346 F.3d 1082, 1088 (Fed. Cir. 2003).

Independent claims 1 and 49 each includes the phrase "application layer information access anomaly." Claim 1 further recites "detecting" such an anomaly by a semantic analysis on a "prototypical model." Claim 49 identifies the anomaly by "performing a semantic analysis against the prototypical model."

The predicate "application layer" in the phase in question distinguishes the anomaly from one that is found at the "network-layer" or "system-layer" (Substitute Specification, at page 5, line 10). Moreover, the adjectival portion "information access" indicates that the "anomaly" is one that arises with respect to or during information retrieval (See, e.g., Substitute Specification, at page 12, lines 8-21). The Substitute Specification further teaches the "idea of correlating content, users, time, and space, and developing trends and detecting anomalies at the information layer." The "information layer" is synonymous with "application layer" as recited in the claim. Thus, the broadest reasonable construction of the phrase "application layer information access anomaly" consistent with the specification (MPEP §2111) is an anomaly that is detected during retrieval of information by users

having access to information." The written description is clear that this phrase is not intended to reach "network-layer" or "system-layer" anomaly detection, nor a mere application layer anomaly that is not related to "information access" per se.

Turning to the rejection, there are several errors justifying **REVERSAL** of the Examiner's rejection of the Group I claims. These claims are rejected under 35 U.S.C. §102(a) "as being clearly anticipated by admissions over the prior arts." (See, Final Rejection, at page 7)

These errors are outlined below.

Anticipation must be proven, not based on arguments "incorporated by reference"

There are several errors justifying **REVERSAL** of the Examiner's rejection of the Group I claims. These claims are rejected under 35 U.S.C. §102(a) "as being clearly anticipated by admissions over the prior arts." (See, Final Rejection, at page 7)

In the first instance, the Examiner's rejection – which attempts to incorporate earlier rejections ("For claims 1-29, 42-45 and 47-49, see the previous Office Actions") – contravenes Rule §1.104(c)(2) which, as noted above, requires that "the pertinence of each [prior art] reference, if not apparent, must be clearly explained." The Examiner does not satisfy this requirement merely by incorporating a prior rejection by reference. Indeed, there is no basis in the Rules, in the MPEP, or in other Office practice or custom for such shorthand. For Rule §104(c)(2) to be satisfied – and it was not here - an Examiner must cite the actual claim language, and then he or she must show how the reference (here, the alleged APA) aligns *with each element of each claim said to be anticipated.* This is so because, as the legal principles above make clear, every element of the claimed invention

must be found in a single prior art reference, arranged as in the claim, the claimed subject matter must be disclosed "clearly and unequivocally" in the reference, picking and choosing isolated teachings in the reference is not permissible, and inherency cannot be based on possibilities or probabilities.

It was error for the Examiner to reject the Group I claims based on "the previous Office Actions."[3] For this reason alone, the rejection should be **REVERSED**.

The Alleged Admitted Prior Art (APA) has been mischaracterized

Moreover, the Examiner errs in characterizing the claimed subject matter in the Group I claims as admitted prior art. No such admission has been made.

In this regard, the gist of the Examiner's position is set forth below (Final Rejection, at page 5):

"The art listed in the specification (at the bibliography in the last pages) amply and redundantly show that prior art did indeed (well known even without page 5 of the specification) already have the Unauthorized Information Disclosure and the Content Usage Analysis as also noted in page 5. Because the prior art did indeed (well known even without page 5) already have the Unauthorized Information Disclosure and the Content Usage Analysis as also noted in page 5, the claims can never be allowed without overcome [sic] the admissions against art at page 5 of the specification of this application."

---

[3] The previous Office actions provide only slightly more substance, but the arguments there (just like the ones here) were never correlated to any actual claim elements. Thus, in the first Office action mailed October 10, 2007, the Examiner cited merely to general statements in the specification regarding "intrusion detection" and "anomaly detection." The second Office action, which was mailed May 11, 2009, argued that "packet analysis, real-time functioning, and changing content" were APA, citing the Bibliography Admission. In this action, the Examiner also contended that several of the claim elements were just reciting "classical" techniques even though the Applicant never stated that this was the case. The third Office action on the merits, which was mailed February 25, 2010, simply reiterated these earlier arguments, as does the Final Rejection here.

The "bibliography" identified by the Examiner refers to thirteen (13) prior art articles that are identified only by their respective title, author, publication date, and source. The specific details of each article are not included in the written description. For convenience, the "bibliography" will be referred to below as the "Bibliography Admission."

The "page 5" admission referred to in the Examiner's above-quoted passage is the following statement from the written description (emphasis supplied): "There have been earlier applications of anomaly detection, but for lower-level activities such as intrusion detection (network-layer or system-layer), or for specific application activity monitoring such as transaction monitoring (credit cards)." For convenience, this sentence will be referred to below as the "Page 5 Admission."

Thus, although the Examiner's reasoning is not entirely clear, he appears to be arguing that the Page 5 Admission, together with the Bibliography Admission, constitutes APA *for each and every limitation* of each Group I claim. With all due respect, this is an erroneous fact finding.

Turning to independent claim 1, and keeping in mind the discussion above concerning claim construction, the APA is unrelated to and does not disclose or suggest "application layer information access anomaly" detection. Rather, at most, the Page 5 Admission references network-layer or system layer anomaly detection, or application activity monitoring detection. The former are unrelated to the application layer, and the latter is unrelated to "information access." The Bibliography Admission adds nothing further to these teachings, as the cited references are only identified by name. Because

"absence from the reference of any claimed element negates anticipation," for this reason alone the APA does not anticipate. *Kloster Speedsteel AB v. Crucible, Inc.*, 793 F.2d 1565, 1571 (Fed.Cir.1986).

Moreover, the Page 5 Admission is not what is being claimed.

Further, and with respect to independent claim 1, the Examiner has not shown how the APA teaches the recited ordered series of steps, *namely:* capturing data packets, filtering the captured data packets to detect information content, processing the packets based on semantics of an application or protocol, deriving a quantitative representation, deriving a content signature, deriving a prototypical model, where the model includes a frequency view of a set of content signatures accessed by a given user, and – finally – *detecting the application layer information access anomaly by using a semantic analysis to detect a given deviation from the prototypical model.*

As is self-evident from the rejection, the Examiner has not even laid out the claim language or shown how the APA is alleged to map to that language. As a consequence, neither the Applicant nor the public has any guidepost to determine whether and to what extent the Examiner's reasoning is correct. In particular, the Examiner has not established where or how the APA (and, in particular, the Page 5 Admission, and/or the Bibliography Admission) are these particular steps, carried out in this sequence. "[E]very limitation positively recited in a claim must be given effect in order to determine what subject matter that claim defines." *In re Wilder*, 429 F.2d 447, 450 (CCPA 1970); *See also In re Wilson*, 424 F. 2d 1382, 1385 (CCPA 1970) ("[a]ll words in a claim must be considered in judging the patentability of that claim against the prior art."). Because the Examiner has not met

the Office's burden to establish that each and every limitation in independent claim 1 – as arranged in the claim - is found in the alleged APA, the rejection must be **REVERSED** on this ground as well.

The same argument applies equally to independent claim 49. In this regard, the Examiner has not shown how or where the APA teaches monitoring data packets indicative of changing content over time, generating a prototypical model, or performing a semantic analysis against the prototypical model to identify the application level information access anomaly. As noted above, the APA concerns network-layer or system-layer anomaly detection, or just application activity (not information access) monitoring. Moreover, the APA is silent regarding generation of a prototypical model that is based on "monitoring data packets indicative of changing content over time," let alone performing any type of analysis on that model to identify the "application layer information access anomaly." The absence of any claim element – and the APA meets none of the recited limitations – dooms the anticipation rejection with respect to this claim as well.

The APA is silent regarding the dependent claimed subject matter

The Examiner states that the "dependent claims recite exactly the features that were asserted as prior art by [the Page 5 Admission]." (See, Final Rejection, at page 8, emphasis in original) With respect, this is incorrect given the limited subject matter set forth in the one sentence upon which the Examiner relies. The following are representative Group I claims, each of which recites subject matter (emphasis supplied) that is *facially* absent from the Page 5 Admission:

"4. The method, according to claim 1, where the quantitative representation is captured as a content distribution vector that captures a frequency based distribution of key words in the message."

6. The method, according to claim 1, where the content signature is computed as a hash of the information content.

7. The method, according to claim 1, where the content signature is computed via a document clustering technique where documents that share content signatures are classified together.

16. The method, according to claim 1, where the information access anomaly is based on a given user accessing given content from a given location at a given time.

17. The method, according to claim 16, where the information access anomaly is detected by a memory-based deviation where the given content accessed by the given user shows a deviation over normal content accessed."

Each dependent claim in Group I likewise includes subject matter absent from the APA, and especially the Page 5 Admission. Because each dependent claim includes at least some absent subject matter, there is no explicit anticipation. Moreover, and as noted above, a claim limitation is inherent in the prior art only if it is "necessarily present in the prior art, not merely probably or possibly present." The Examiner has made no such showing, and he does not argue inherency either.

Thus, with respect to the dependent claims, the Examiner has not shown anticipation.

Anticipation must be established for each claim, element-by-element

The prior art set forth in the written description might well be deemed "admitted prior art," but what matters here is whether the admitted prior art "reads on" the claimed invention, which it does not, for at least the reasons set forth above. Applicant is not seeking to patent the alleged APA, and (at the very least) the following subject matter is not APA:

Claim 1:

"processing packets based on semantics of an application or protocol;"

"generating a quantitative representation;"

"deriving a content signature from the quantitative representation;"

"deriving a prototypical model that includes a frequency view of a set of content signatures accessed by a given user, where the set of content signatures are indicative of content that is changing over time; and

"detecting an application layer information access anomaly by using a semantic analysis to detect a given deviation from the prototypical model."

Claim 49:

"monitoring data packets indicative of changing content over time;

generating a prototypical model; and

performing a semantic analysis against the prototypical model to identify an application level information access anomaly."

To establish anticipation, every element and limitation of the claimed invention must be found in a single prior art reference, arranged as in the claim. *Karsten Mfg. Corp. v. Cleveland Golf Co*., 242 F.3d 1376, 1383 (Fed. Cir. 2001)

"Absence from the reference of any claimed element negates anticipation." *Kloster Speedsteel AB v. Crucible, Inc.*, 793 F.2d 1565, 1571 (Fed.Cir.1986).

Here, and with respect, the Examiner has not shown how either claim 1 or claim 49 is anticipated.

Further, the Applicant has not admitted that the subject matter of the dependent claims is admitted prior art.

Thus, the rejection of the Group I claims should be **REVERSED**.

Group II – claims 52-53

These dependent claims further require that the semantic analysis examine an "entirety of an application layer without any application-specific limits." The genesis of this clause was the Examiner's suggestion (in the Office action mailed February 25, 2010, at pages 5-6) and, in particular, a statement to the effect that the claims might be allowable if this subject matter were recited. Because there was adequate support for the limitation in the specification, the Applicant elected to take the Examiner up on the suggestion, and the dependent claims 52-53 were added into the case.

Despite including the limitation, however, the Final Rejection (at page 5, last sentence in the full paragraph) states "At the moment, none of the claims have yet to claim any of this subject matter." With respect, the Examiner's contention is inexplicable. The very subject matter that the Examiner indicates should be recited *has been included*.

Moreover, it must be the case (and it is) that the APA does not recite this subject matter, as otherwise the Examiner would not have suggested its inclusion.

For the same reasons as advanced above with respect to the Group I claims, and for the further reason that the "entirety of an application layer" clause is absent from the APA (given the Examiner's explicit suggestion to include it, which Applicant has done), the Group II claims also are neither explicitly nor inherently taught by the APA.

Thus, the rejection of the Group II claims likewise should be **REVERSED**.

* * *

The Examiner has indicated on several occasions that there is allowable subject matter in this case, and there is. The Final Rejection (at page 5-7) even includes a proposed claim template that the Examiner suggests might be the basis of something allowable ("at the minimum"). While the Applicant appreciates the Examiner's consideration is this regard, the Applicant is entitled to present claims that are believed patentable over the actual prior art (not illusory APA), and it is the Office's burden to show otherwise. The Applicant does not bear any burden to show that the claims are not anticipated; that is and remains the Office's obligation in the first instance.

Here, and with all due respect, the Final Rejection does not meet the Office's burden to establish anticipation of the *claimed subject matter*. **REVERSAL** is mandated in these circumstances.

Respectfully submitted,

By: /David H. Judson/
David H. Judson, Reg. No. 30,467

May 30, 2011

(viii) Claims Appendix.

1. A method of performing an application layer semantic analysis to detect information access anomalies, comprising:

a) capturing data packets;

b) filtering the captured data packets to detect information content;

c) processing packets based on semantics of an application or protocol;

d) generating a quantitative representation;

e) deriving a content signature from the quantitative representation;

f) deriving a prototypical model that includes a frequency view of a set of content signatures accessed by a given user, where the set of content signatures are indicative of content that is changing over time; and

g) detecting an application layer information access anomaly by using a semantic analysis to detect a given deviation from the prototypical model.

2. The method, according to claim 1, where the prototypical model also includes a time distribution of a set of content accesses by the given user.

3. The method, according to claim 1, where the prototypical model also includes a location distribution of a set of content accesses by the given user.

4. The method, according to claim 1, where the quantitative representation is captured as a content distribution vector that captures a frequency based distribution of key

words in the message.

5. The method, according to claim 1, where the content signature is computed based on a moment statistic.

6. The method, according to claim 1, where the content signature is computed as a hash of the information content.

7. The method, according to claim 1, where the content signature is computed via a document clustering technique where documents that share content signatures are classified together.

8. The method, according to claim 1, further including storing the information content, the content signature, and one or more attributes, where the attributes include one of: user identity, location of access, time of access, content type, content length, content hash, content encoding, and one or more content properties.

9. The method, according to claim 1, where mining is based on statistical clustering and distance based metrics.

10. The method, according to claim 9, where a statistical metric includes frequency of all content signatures accessed by a user.

11. The method, according to claim 9, where a statistical metric includes time of all content signatures accessed by a user.

12. The method, according to claim 9, where a statistical metric includes location of all content signatures accessed by a user.

13. The method, according to claim 1, where the prototypical model is derived by mining a content database.

14. The method, according to claim 1, where mining may be augmented by content aging, where information is periodically deleted from the content database.

15. The method, according to claim 14, where content aging is a function of a mining algorithm and a type of information being monitored.

16. The method, according to claim 1, where the information access anomaly is based on a given user accessing given content from a given location at a given time.

17. The method, according to claim 16, where the information access anomaly is detected by a memory-based deviation where the given content accessed by the given user shows a deviation over normal content accessed.

18. The method, according to claim 16, where the information access anomaly is detected by a rare content condition, where the given user accesses given content that is rarely accessed by the given user.

19. The method, according to claim 16, where the information access anomaly is detected by a time deviation where the given user accesses the given content at a time different from historical access by the given user.

20. The method, according to claim 16, where the information access anomaly is detected by a location deviation where the given user accesses the given content from a location different from historical access by the given user.

21. The method, according to claim 1, further including processing the information access anomaly.

22. The method, according to claim 21, where processing the information access anomaly processing includes one of: positive correlation with at least one past security violation event, and negative correlation with a past false alarm or non-event.

23. The method, according to claim 1, where a set of consistent anomalies are classified into a pattern of misuse.

24. The method, according to claim 1, where the information access anomaly is detected in real-time.

25. The method, according to claim 1, where information access anomaly detection is used for real-time protection of information.

26. The method, according to claim 25, where real-time anomaly detection is used for protection via real-time alerts.

27. The method, according to claim 25, where real-time anomaly detection is used for real- time protection via denial of access.

28. The method, according to claim 25, where real-time anomaly detection is used for real- time protection via additional user validation.

29. The method as described in claim 1, where the data packets are associated with access to a confidential information repository.

30-41. (cancelled)

42. The apparatus of claim 49, implemented on a computing device and connected on a network as a passive tap.

43. The apparatus of claim 49, implemented as a network appliance that derives information transparently.

44. The apparatus of claim 49, implemented on an end-user computing device.

45. The apparatus of claim 49, implemented as a shim on an application server.

46. (cancelled)

47. The apparatus of claim 49, connected to an access control system to enable real-time monitoring of anomalous information access.

48. The apparatus of claim 49, configured to implement one or more compliance policies.

49. Apparatus, comprising:

a processor; and

a computer memory storing program instructions that when executed by the processor perform a method of detecting an information access anomaly, the method comprising:

monitoring data packets indicative of changing content over time;

generating a prototypical model; and

performing a semantic analysis against the prototypical model to identify an application level information access anomaly.

50. (cancelled)

51. (cancelled)

52. The method of claim 1 wherein the application layer semantic analysis examines an entirety of an application layer without any application-specific limits.

53. The apparatus as described in claim 49 wherein the detecting method examines an entirely of an application layer without any application-specific limits.

(ix) Evidence Appendix.

None.

(x) Related Proceeding Appendix.

None.